LE MATEMATICHE
Vol. LXVIII (2013) – Fasc. I, pp. 3–11
doi: 10.4418/2013.68.1.1

COMPUTATIONS IN MULTIVARIATE QUATERNIONIC POLYNOMIAL RING

DANG TUAN HIEP

In this paper we study division algorithm and Gröbner bases in the multivariate quaternionic polynomial ring.

1. Multivariate quaternionic polynomial ring

Let $\mathbb{H}$ denote the algebra of real quaternions. This algebra is generated by three elements i, j, k, called imaginary units since they satisfy the relations $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i$, and $ki = -ik = j$. The elements in $\mathbb{H}$ can be written as $q = x_0 + ix_1 + jx_2 + kx_3$ where x_0, x_1, x_2 and x_3 are real. Then we also define $\overline{q} = x_0 - ix_1 - jx_2 - kx_3$ and check easily that

$$q\overline{q} = \overline{q}q = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{R}.$$

Thus, if $q \neq 0$ then $q^{-1} = (x_0^2 + x_1^2 + x_2^2 + x_3^2)^{-1}\overline{q}$. In particular, $\mathbb{H}$ is a four–dimensional division algebra over $\mathbb{R}$.

Technically, polynomials over the quaternions could be finite sums of elements of the type $aq_1^{\alpha_1} \dots q_n^{\alpha_n}$ or $q_1^{\alpha_1} \dots q_n^{\alpha_n} a$, with $a \in \mathbb{H}$, or, more in general, words of the type

$$a_0 q_1^{\alpha_1} \dots q_n^{\alpha_n} a_1 q_1^{\beta_1} \dots q_n^{\beta_n} \dots a_{k-1} q_1^{\gamma_1} \dots q_n^{\gamma_n} a_k,$$

Entrato in redazione: 30 luglio 2011

AMS 2010 Subject Classification: 13P10, 17C60, 68W30.
Keywords: Quaternionic polynomials, Division algorithm, Gröbner bases, Noncommutative rings.
Partly sponosered by Università degli Studi di Bari Aldo Moro.

with $a_l \in \mathbb{H}$. However, we only focus on the powers of $q_1, \ldots, q_n$ with left coefficients in $\mathbb{H}$.

Definition 1.1. The ring of multivariate quaternionic polynomials $\mathbb{H}[q_1, \ldots, q_n]$ is the set whose elements are of the type

$$\sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_\alpha q_1^{\alpha_1} \ldots q_n^{\alpha_n},$$

where $a_\alpha \in \mathbb{H}$, endowed with the noncommutative product defined by the linear extension of

$$(a_\alpha q_1^{\alpha_1} \ldots q_n^{\alpha_n}) * (a_\beta q_1^{\beta_1} \ldots q_n^{\beta_n}) = a_\alpha a_\beta q_1^{\alpha_1+\beta_1} \ldots q_n^{\alpha_n+\beta_n}.$$

As in every noncommutative ring, ideals of $\mathbb{H}[q_1, \ldots, q_n]$ can be left, right or bilateral, depending on which side one allows multiplication. For the sake of simplicity, most of the times we will consider left ideals only. Unless otherwise specified, our results on left ideals will translate into the corresponding ones for right ideals in a straightforward manner.

2. Division algorithm and Gröbner bases

In [2], the authors showed that the ring of one variable quaternionic polynomials $\mathbb{H}[q]$ be an (left or right) Euclidean domain.

Proposition 2.1 (Euclidean Division)**.** *Let $F, G \in \mathbb{H}[q]$ with $\deg(G) > 0$. Then there exist Q, R, Q' and R' in $\mathbb{H}[q]$, with $\max(\deg(R), \deg(R')) < \deg(G)$, such that*

$$F = Q * G + R \ \text{ and } \ F = G * Q' + R'.$$

Moreover, such polynomials are uniquely determined.

Then they gave an algorithm for the calculation of the greatest common divisor using Euclidean division and proved immediately the following corollary.

Corollary 2.2. *Every left or right ideal of $\mathbb{H}[q]$ is principal.*

Thus, in the ring of one variable quaternionic polynomials, division algorithm and stucture of the left or right ideals look like as in the ring of polynomials with coefficients over a field. In order to do calculations we need a system for ordering the terms of a polynomial. For polynomials in one variable, the natural order is by degree, i.e.,

$$q^m > q^n \quad \text{if} \quad m > n.$$

However, for polynomials in many variables, we have seen that the order is essentially arbitrary. We first fix terminology. Given a polynomial

$$\sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_\alpha q_1^{\alpha_1}\ldots q_n^{\alpha_n},$$

with $a_\alpha \in \mathbb{H}$, each $a_\alpha q_1^{\alpha_1}\ldots q_n^{\alpha_n}$ is a term. A polynomial of the form

$$q^\alpha = q_1^{\alpha_1}\ldots q_n^{\alpha_n}$$

is called a monomial.

Definition 2.3. A monomial order $>$ on $\mathbb{H}[q_1,\ldots,q_n]$ is a total order on monomials satisfying the following:

(i) If $q^\alpha > q^\beta$ then $q^\alpha q^\gamma > q^\beta q^\gamma$ (for any α,β,γ).

(ii) An arbitrary set of monomials $\{q^\alpha\}_{\alpha\in A}$ has a least element.

We give a basic example of monomial orders:

Example 2.4 (Lexicographic order)**.** This is basically the order on words in a dictionary. We have $q^\alpha >_{\text{lex}} q^\beta$ if the first nonzero entry of $(\alpha_1-\beta_1,\ldots,\alpha_n-\beta_n)$ is positive. For example, we have

$$q_1 >_{\text{lex}} q_2^3 >_{\text{lex}} q_2q_3 >_{\text{lex}} q_3^5.$$

It is easy to prove this is a monomial order.

Definition 2.5. Fix a monomial order on $\mathbb{H}[q_1\ldots,q_n]$ and consider a nonzero polynomial

$$f = \sum_\alpha a_\alpha q^\alpha.$$

The leading monomial of f (denoted $\text{LM}(f)$) is the largest monomial q^α such that $a_\alpha \neq 0$. The leading term of f (denoted $\text{LT}(f)$) is the corresponding term $a_\alpha q^\alpha$.

Definition 2.6. We say that a left (resp. right) ideal is finitely generated if there is a finite set of nonzero polynomials $f_1,\ldots,f_r \in \mathbb{H}[q_1,\ldots,q_n]$ such that each $g \in I$ has a representation

$$g = h_1 * f_1 + \cdots + h_r * f_r \quad (\text{resp. } g = f_1 * h_1 + \cdots + f_r * h_r),$$

where $h_1,\ldots,h_r \in \mathbb{H}[q_1,\ldots,q_n]$. Then we denote

$$I = \langle f_1,\ldots,f_r\rangle_l \text{ (resp. } I = \langle f_1,\ldots,f_r\rangle_r).$$

Definition 2.7. Let $f, g \in \mathbb{H}[q_1, \ldots, q_n]$. We say that f divides g on the left (resp. on the right) if there exists $h \in \mathbb{H}[q_1, \ldots, q_n]$ such that $g = h * f$ (resp. $g = f * h$). Then we denote $h = g/f$.

Algorithm 2.8 (Division algorithm)**.** Fix a monomial order $>$ on $\mathbb{H}[q_1, \ldots, q_n]$ and nonzero polynomials $f_1, \ldots, f_r \in \mathbb{H}[q_1, \ldots, q_n]$. Given $g \in \mathbb{H}[q_1, \ldots, q_n]$, we want to determine whether $g \in \langle f_1, \ldots, f_r \rangle_l$:

Step 0. Put $g_0 = g$. If there exists no f_j with $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(g_0)$ on the left then we stop. Otherwise, pick such an f_{j_0} and cancel leading terms by putting

$$g_1 = g_0 - (\mathrm{LT}(g_0)/\mathrm{LT}(f_{j_0})) * f_{j_0}.$$

...

Step i. Given g_i, if there exists no f_j with $\mathrm{LM}(f_j)$ divides $\mathrm{LM}(g_i)$ on the left then we stop. Otherwise, pick such an f_{j_i} and cancel leading terms by putting

$$g_{i+1} = g_i - (\mathrm{LT}(g_i)/\mathrm{LT}(f_{j_i})) * f_{j_i}. \tag{1}$$

As we are cancelling leading terms at each stage, we have

$$\mathrm{LM}(g) = \mathrm{LM}(g_0) > \mathrm{LM}(g_1) > \cdots > \mathrm{LM}(g_i) > \mathrm{LM}(g_{i+1}) > \cdots.$$

By the well-ordering property of the monomial order, such a chain of decreasing monomials must eventually terminate. If this algorithm does not stop, then we must have $g_N = 0$ for some N. Back-substituting using equation (1), we obtain

$$\begin{aligned} g &= \sum_{i=0}^{N-1} (\mathrm{LT}(g_i)/\mathrm{LT}(f_{j_i})) * f_{j_i} \\ &= \sum_{j=1}^{r} \left(\sum_{j_i = j} (\mathrm{LT}(g_i)/\mathrm{LT}(f_{j_i})) \right) * f_j \\ &= \sum_{j=1}^{r} h_j * f_j. \end{aligned}$$

Unfortunately, this algorithm often stops prematurely. Even when

$$g \in \langle f_1, \ldots, f_r \rangle_l,$$

it may happen that $\mathrm{LM}(g)$ is not divisible by any $\mathrm{LM}(f_j)$.

Example 2.9. Let $f_1 = (1 + i + 2k)q - i, f_2 = (2i + j)q$ and $g = 1$. We certainly have $g \in \langle f_1, f_2 \rangle_l$ but $\mathrm{LM}(g)$ is not divisible by $\mathrm{LM}(f_1)$ or $\mathrm{LM}(f_2)$, so the procedure stops at the initial step.

To understand better why this breakdown occurs, we make the following definitions:

Definition 2.10. A left (resp. right) monomial ideal $I \subset \mathbb{H}[q_1,\dots,q_n]$ is a left (resp. right) ideal generated by a collection of monomials $\{x^\alpha\}_{\alpha\in A}$. Fix a monomial order $>$ and let $I \subset \mathbb{H}[q_1,\dots,q_n]$ be a left (resp. right) ideal. We denote $\mathrm{LLT}(I)$ (resp. $\mathrm{RLT}(I)$) the left (resp. right) monomial ideal generated by leading terms of the polynomials in I.

Definition 2.11 (Gröbner bases)**.** Fix a monomial order $>$ and let

$$I \subset \mathbb{H}[q_1,\dots,q_n],$$

be a left (resp. right) ideal. A left (resp. right) Gröbner basis for I is a collection of nonzero polynomials $\{f_1,\dots,f_r\} \subset I$ such that $\mathrm{LT}(f_1),\dots,\mathrm{LT}(f_r)$ generate $\mathrm{LLT}(I)$ (resp. $\mathrm{RLT}(I)$)).

Nothing in Definition 2.11 says that a left Gröbner basis actually generates I. We prove this is also true later.

Remark 2.12. In the one variable case, every generator for a left (resp. right) principal ideal is a left (resp. right) Gröbner basis.

Proposition 2.13. *Let $I \subset \mathbb{H}[q_1,\dots,q_n]$ be a left ideal and $\{f_1,\dots,f_r\}$ be a left Gröbner basis for I. The division algorithm terminates in a finite number of steps, with either $g_i = 0$ or $\mathrm{LT}(g_i)$ not divisible by any of the leading terms $\mathrm{LT}(f_j)$.*

1. *In the first case, the algorithm returns a representation*

$$g = h_1 * f_1 + \cdots + h_r * f_r,$$

where $h_j \in \mathbb{H}[q_1,\dots,q_n]$, and $g \in I$.

2. *In the second case, we obtain an expression*

$$g = h_1 * f_1 + \cdots + h_r * f_r + g_i,$$

where $\mathrm{LT}(g_i) \notin \langle \mathrm{LT}(f_1),\dots,\mathrm{LT}(f_r)\rangle_l$, hence $g \notin I$.

This proposition immediately implies the following corollary.

Corollary 2.14. *Fix a monomial order $>$. Let $I \subset \mathbb{H}[q_1,\dots,q_n]$ be a left ideal and $\{f_1,\dots,f_r\}$ be a left Gröbner basis for I. Then $I = \langle f_1,\dots,f_r\rangle_l$.*

The proof of Proposition 2.13 will use the following lemma.

Lemma 2.15. *Let I be a left monomial ideal generated by a collection of monomials $\{q^\alpha\}_{\alpha\in A}$. Then every monomial in I is a left multiple of some q^α.*

Proof. Let q^β be a monomial in I. Then we can write

$$q^\beta = \sum_i w_i * q^{\alpha(i)},$$

where the w_i are polynomials. In particular, q^β appears in the right-hand side and hence it is a monomial of $w_i * q^{\alpha(i)}$ for some i. Thus it is divisible by $q^{\alpha(i)}$ on the left. □

Proof of Proposition 2.13. We have already shown that we obtain a representation

$$g = h_1 * f_1 + \cdots + h_r * f_r$$

unless the algorithm stops. We need to show the algorithm terminates with $g_i = 0$ for some i whenever $g \in I$. If $g \in I$ then the intermediate $g_i \in I$ as well. We now use the definition of a left Gröbner basis: If, for some i, the leading term $\mathrm{LT}(g_i)$ is not divisible by $\mathrm{LT}(f_j)$ for any j, then

$$\mathrm{LT}(g_i) \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r)\rangle_l$$

by Lemma 2.15. It follows that $g_i \notin I$; the formula relating g and g_i guarantees that $g \notin I$. □

3. Existence of Gröbner bases

We have not yet established that left (resp. right) Gröbner bases exist, or even that each left (resp. right) ideal of $\mathbb{H}[q_1, \ldots, q_n]$ is finitely generated. In this section, we shall prove the following theorem.

Theorem 3.1 (Existence Theorem)**.** *Fix a monomial order $>$ and a nonzero left (resp. right) ideal $I \subset \mathbb{H}[q_1, \ldots, q_n]$. Then I admits a finite left (resp. right) Gröbner basis.*

Corollary 3.2. *Every left (resp. right) ideal in multivariate quaternionic polynomial ring is finitely generated.*

It suffices to show that $\mathrm{LLT}(I)$ is finitely generated. Indeed, if $f_1, \ldots, f_r \in I$ are chosen such that

$$\mathrm{LLT}(I) = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r)\rangle_l$$

then Corollary 2.14 implies

$$I = \langle f_1, \ldots, f_r \rangle_l.$$

Thus the proof of the existence theorem is reduced to the case of left (resp. right) monomial ideals:

Proposition 3.3. *Every left (resp. right) monomial ideal in a multivariate quaternionic polynomial ring is generated by a finite collection of monomials.*

Proof. Let $I \subset \mathbb{H}[q_1, \ldots, q_n]$ be a left monomial ideal. We want to find a finite number of monomials in I generating I. The proof is by induction on n, the number of variables. If $n = 1$, by Corollary 2.2, every left ideal in $\mathbb{H}[q_1]$ is principal: If q_1^α is the monomial of minimal degree in I and $q_1^\beta \in I$, then $\alpha \leq \beta$ and $q_1^\alpha \mid q_1^\beta$. For the inductive step, we assume the result is valid for $\mathbb{H}[q_1, \ldots, q_n]$ and deduce it for $\mathbb{H}[q_1, \ldots, q_n, q_{n+1}]$. Consider the following set of auxiliary left monomial ideals $I_m \subset \mathbb{H}[q_1, \ldots, q_n]$:

$$I_m = \langle q^\alpha \in \mathbb{H}[q_1, \ldots, q_n] \mid q^\alpha q_{n+1}^m \in I \rangle_l.$$

Note that we have an ascending chain of left monomial ideals:

$$I_0 \subset I_1 \subset I_2 \subset \cdots I_m \subset I_{m+1} \subset \cdots.$$

Consider

$$I_\infty = \bigcup_m I_m,$$

which is also a left monomial ideal in $\mathbb{H}[q_1, \ldots, q_n]$. By inductive assumption, $I_\infty = \langle g_1, \ldots, g_r \rangle_l$. Each $g_i \in I_{n_i}$ for some n_i. If $N = \max(n_1, \ldots, n_r)$ then $I_\infty = I_N$. The sequence of left monomial ideals $I_m \subset \mathbb{H}[q_1, \ldots, q_n]$ terminates at some I_N. Therefore, there is a finite sequence of monomials:

$$\begin{gathered}
\langle q^{\alpha(0,1)}, \ldots, q^{\alpha(0,n_0)} \rangle_l = I_0 \\
\langle q^{\alpha(1,1)}, \ldots, q^{\alpha(1,n_1)} \rangle_l = I_1 \\
\vdots \\
\langle q^{\alpha(N,1)}, \ldots, q^{\alpha(N,n_N)} \rangle_l = I_N
\end{gathered}$$

generating each of the I_m for $m \geq N$. The left monomial ideal I is therefore generated by the terms $q^{\alpha(m,j)} q_{n+1}^m$ for $m = 0, \ldots, N; j = 1, \ldots, n_m$. □

Let $\mathcal{H}$ be the $\mathbb{R}-$algebra generated by $i, j, k, q_1, \ldots, q_n$ and satisfying the following relations

(a) $q_t q_s = q_s q_t$ for all $1 \leq s < t \leq n$,

(b) $q_s i = i q_s, q_s j = j q_s, q_s k = k q_s$ for all $1 \leq s \leq n$,

(c) $ji = -ij, kj = -jk, ki = -ik$.

Notice that the relations of (c) in the above proposition make i, j and k into anti-commutative variables, while (a) and (b) say that $q_1, \ldots, q_n$ behave like n variables in a multivariate commutative polynomial ring. Let I be the two-sided ideal of $\mathcal{H}$ generated by $i^2+1, j^2+1, k^2+1, ij-k, jk-i, ik+j$. We can state the next result.

Proposition 3.4. $\mathbb{H}[q_1, \ldots, q_n] \simeq \mathcal{H}/I$.

We omit its proof since it is straightforward.
Since $\mathbb{H}[q_1, \ldots, q_n]$ is a quotient of the $\mathbb{R}-$algebra $\mathcal{H}$, every left (resp. right) ideal admits a left (resp. right) Gröbner basis.

4. Computations using SINGULAR

If we use SINGULAR, the ring $\mathbb{H}[q_1, \ldots, q_n]$ can be introduced via a sequence of commands. For instance, if $n = 2$, the ring of the quaternionic polynomials in two variables can be defined as follows.

```
> ring r=0,(x,y,i,j,k),lp;
> matrix C[5][5] = 0,1,1,1,1,0,0,1,1,1,0,0,0,-1,-1,
                   0,0,0,0,-1,0,0,0,0,0;
> ncalgebra(C,0);
> ideal I=i2+1,j2+1,k2+1,ij-k,jk-i,ik+j;
> qring H=twostd(I);
```

Note that, where x, y are two variables and i, j, k are three imaginary units in $\mathbb{H}$.

Let $f_1 = ix + jy$ and $f_2 = kx + iy$ are two polynomials in $\mathbb{H}[x, y]$, then we can compute the left Gröbner basis for left ideal generated by f_1, f_2 via the following commands.

```
> setring H;
> option(redSB);
> option(redTail);
> ideal b=ix+jy,kx+iy;
> ideal I=std(b);
> I;
//-> I[1]=y
//-> I[2]=x
```

Remark 4.1. After computing, the results will give the polynomials with the right coefficients. So we must take the same polynomials with the left coefficients. For instance, let us compute the left Gröbner basis for left ideal generated by $g_1 = ix^4 + jxy^3, g_2 = kx^3 + iy^2$.

```
> ideal c=ix4+jxy3,kx3+iy2;
> ideal J=std(c);
> J;
//-> J[1]=y4
//-> J[2]=xy2
//-> J[3]=x3-y2j
```

This means that $\{y^4, xy^2, x^3 - jy^2\}$ is a left Gröbner basis for the left ideal $\langle g_1, g_2 \rangle_l$.

Acknowledgment

The author is grateful to Università degli Studi di Bari Aldo Moro for the financial support during the period in which this paper was written.

REFERENCES

[1] D. Cox - J. Little - D. O'Shea, *Ideals, varieties and algorithms: An introduction to computational algebraic geometry and commutative algebra*, Springer, second edition, 1997.

[2] A. Damiano - G. Gentili - D. Struppa, *Computations in the ring of quaternionic polynomials*, Journal of Symbolic Computation 45 (2010), 38–45.

[3] G. Gentili - C. Stoppato - D. C. Struppa, *Regular functions of a quaternionic variable*, Springer, 2013.

[4] G-M. Greuel - G. Pfister, *A* SINGULAR *Introduction to commutative algebra*, Springer, 2008.

[5] W. Decker - G-M. Greuel - G. Pfister - H. Schönemann, SINGULAR *3-1-4 — A computer algebra system for polynomial computations*, 2012, available at `http://www.singular.uni-kl.de`.

[6] T. Y. Lam, *A first course in noncommutative rings*, Springer, 1991.

[7] V. Levandovskyy, *Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation*, PhD thesis, University of Kaiserslautern, 2005.

DANG TUAN HIEP
Università di Bari, Dipartimento di Matematica
Via Orabona, 4 - 70125 Bari, Italy
e-mail: `dang@dm.uniba.it`